GenoBank.io™

TECHNICAL WHITEPAPER · ETHEREUM STANDARDS · CONSENT INFRASTRUCTURE

ERC-8356: Purpose-Bound Third-Party Data Consent

A Standards Track proposal for revocable, purpose-bound consent grants in which the consenting subject is not the beneficiary, with an independently revocable agent leg. Status anchors on-chain. Instruments off-chain. Withdrawal that works at access time.

AUTHOR

Daniel Uribe, Founder and CEO, GenoBank.io

DATE

August 1, 2026

STANDARD

ERC-8356 (Draft), ethereum/ERCs #1921

DISCUSSION

Ethereum Magicians #29217

STACK

GenoBank.io · Sequentia · Metamorphic Consent

VERSION

1.0

Status. Draft · ethereum/ERCs #1921 · CI green as of 2026-08-01 · labels: `s-draft`, `e-review`. This whitepaper exposits a draft Standards Track proposal; it is not a Final ERC.

3 PRINCIPALS PER GRANT	**48** REFERENCE TESTS
3	**O(1)**

CHAINS DEPLOYED	REVOCATION COST

1. Abstract

This whitepaper presents **ERC-8356: Purpose-Bound Third-Party Data Consent**, a Standards Track Ethereum Request for Comment authored by Daniel Uribe and opened as ethereum/ERCs pull request 1921. The standard defines a consent grant in which three principals are distinguished: a **subject** who consents, a **grantee** who receives access, and an optional **agent** that acts on the grantee's behalf. The subject is not the beneficiary. The grant is bound to a declared purpose drawn from a versioned code registry, carries a validity window and a usage cap, may be attenuated into sub-grants that can never exceed their parent, and can be revoked either in whole by the subject or in part by terminating only the agent leg.

The on-chain record is a **status anchor**, not the instrument. The instrument, the human-readable authorization the subject actually assented to, remains off-chain and is referenced by hash. What the chain contributes is public, non-repudiable, consensus-ordered revocation, and the ability to prove that a grant existed before a given access. That separation is deliberate: it is the only design that is simultaneously honest about what a smart contract can and cannot observe, compatible with GDPR Article 17 erasure arguments, and useful to a relying party that must refuse access when consent has been withdrawn.

We situate ERC-8356 in the GenoBank.io stack (BioNFT, BioFS, Sequentia chain 15132025, Metamorphic Consent) and in the broader Ethereum agent and compliance landscape (ERC-8226, ERC-8328, ERC-8004, ERC-4907, ERC-5006). We also document the concrete gap in the incumbent non-blockchain practice for controlled genomic datasets, the GA4GH Authentication and Authorization Infrastructure profile, whose revocation propagation is bounded by token lifetime and hourly polling. A withdrawal that takes an hour to reach the gate is a poor fit for legal regimes whose operative triggers are knowledge and ease of withdrawal.

A reference implementation of the ConsentGrant contract has been deployed, tested (48 tests, mostly negative), and verified on Avalanche and Sequentia. The paper closes with deployment

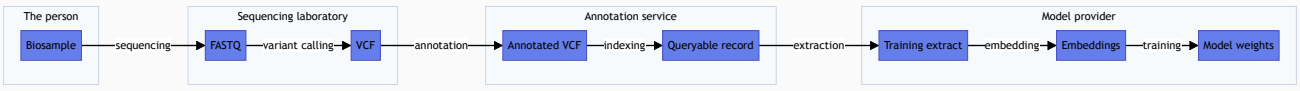
addresses, open items that remain deliberately honest rather than papered over, and a research agenda for purpose ontologies, off-chain enforcement composition, and agent identity registries.

2. The Three-Party Consent Problem

Delegated access to regulated data is now routinely exercised by software agents acting for a human principal. A clinician opens a chart through a hospital portal. A research fellow downloads a VCF through an MCP tool bound to a laboratory account. A model training pipeline ingests embeddings derived from a patient cohort. In each case the person whose body the data describes is rarely the party who holds the session key, and is never the party who benefits from the access. The consenting subject and the economic or scientific beneficiary are different people. That is the shape of consent to use data about a person, and it is the shape that every major on-chain delegation standard currently fails to express.

A datum about a person is rarely a single object. It is a chain of derived artifacts, each produced by a different custodian and each further from the person than the last. A biological sample is the clearest case, and it is the case GenoBank.io was built to govern. A biosample becomes FASTQ under a sequencing laboratory, becomes VCF under a variant caller, becomes an annotated VCF under an annotation service, becomes a queryable record under a clinical or research store, becomes a training extract under a model provider, becomes embeddings, and finally becomes model weights. One consent decision at the left of that chain is asked to govern seven transformations across four custodians, and the person is asked again at none of them.

FIGURE 1. METAMORPHOSIS OF A BIOSAMPLE INTO IRREVERSIBLE MODEL ARTIFACTS



TEXT SUMMARY (FIGURE 1)

Biosample transforms left to right: Sample to FASTQ to VCF under a sequencing laboratory; annotated VCF and queryable record under an annotation service; training extract, embeddings, and model weights under a model provider. Each hop is a new custodian. Deletion remains available until model weights, where only measurement and accounting remain.

Two properties follow from that graph, and no existing Standards Track ERC provides either. The permission must compose along the chain, narrowing at each hop and never widening. And withdrawal must run the chain in reverse, which it can do until it reaches model weights, where deletion is not available and only measurement and accounting remain. GenoBank.io's Metamorphic Consent thesis is that consent is not a static permission form. It is an ongoing economic and technical relationship that must be enforceable at access time, revocable without the cooperation of the party that benefits, and honest about the hard edge where deletion fails.

The three principals of ERC-8356 map onto that graph without distortion. The **subject** is the natural person whose data the grant concerns. The **grantee** is the laboratory, researcher, or institution authorized to exercise the grant. The **agent** is the session key, tool provider, or model runtime that exercises the grant on the grantee's behalf. Collapsing any two of those roles into one is how existing standards produce an audit trail that looks authoritative and is not.

3. Why Existing Delegation Standards Are Two-Party

Every delegation standard currently on the Standards Track is two-party: the principal who signs is the principal who benefits, and the asset at risk is the principal's own. In ERC-4907 and ERC-5006 a token owner grants a time-boxed user role over their own token. In ERC-8226 a principal delegates scoped, capped authority to an agent over the principal's own asset, with the mandate keyed (agent, principal). In every case the party who consents is the party who benefits, and the party at risk is the party who signed. The case this whitepaper addresses is structurally different: a subject consents to a grantee's access to data about the subject, and the harm from an unauthorized act falls on someone who is not a party to the transaction at all.

Other standards do model a subject. ERC-8328 defines subjectId, ROLE_SUBJECT, and ROLE_BENEFICIARY. W3C Verifiable Credentials 2.0 separates credentialSubject from holder and issuer. What neither does is make that non-party subject's withdrawal **operative for a relying party at access time**. ERC-8328 says so itself: it does not define compliance policy or transfer restrictions, and its OUTCOME_REVOKED is a recorded assertion that nothing consults. Recording that a subject asked to leave is not the same as forcing every gate that reads the grant to refuse. That is the gap ERC-8356 closes, and it is the whole of the claim.

Where an agent is modeled at all in prior work, it is modeled as an extension of the principal. There is no way to say "this researcher retains access, but the tool they were using does not," which is precisely the action an incident response requires when a model provider, an MCP server, or a session key is compromised. Purpose is not enforced anywhere on the Standards Track. Every regulatory-compliance ERC to date (ERC-3643, ERC-7518, ERC-8106, ERC-8226, ERC-8320) encodes securities and real-world-asset vocabulary: accreditation, jurisdiction blocks, AML flags, transfer caps. A fund unit has no purpose limitation, so the vocabulary was never needed. Data has one.

> **DESIGN CLAIM**
>
> If the party who consents is not the party who benefits, two-party delegation is the wrong abstraction. Profiles of ERC-8226 cannot be stretched to hold a third principal without rewriting the mandate key, the compliance timing, and the normative status of metadata. Composition is the right relationship: an agent may hold an ERC-8226 mandate over a payment asset and a grant under ERC-8356 over a data asset.

The 2020 paper by Entriken and Uribe, "Biosample permission token with non-fungible tokens," already set out the permitter, permitee, and permit model that GenoBank.io builds on, using ERC-721 to publish permit status and to resolve a permit recursively back to the property owner. It established the three-role framing and the public-status requirement. What it did not do is bind a permit to a declared purpose, give the agent an independently revocable leg, or make the permitter's withdrawal operative for a relying party at access time. Those three additions are what ERC-8356 contributes as a Standards Track proposal rather than as a proprietary GenoBank.io interface.

4. The GA4GH AAI Gap: Hourly Polling Is Not Withdrawal

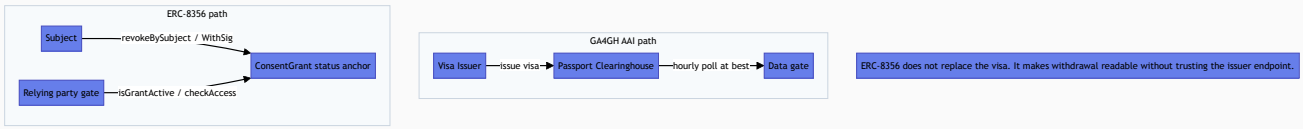
The incumbent non-blockchain mechanism for credentialed access to controlled genomic datasets is the GA4GH Authentication and Authorization Infrastructure profile. It is widely deployed, carefully reviewed, and intentionally designed for federation across passport clearinghouses. It is also honest, in its own text, about the limits of its revocation model. A Visa Issuer "MAY provide tokens of this type without any revocation process." The profile defines exp as explicitly not a hard cutoff, noting that access "is NOT necessarily removed by the exp

timestamp." The only active validity check is rate-limited: polling "MUST NOT be done more than once per hour per Passport Clearinghouse." There is no revocation list and no push mechanism. Worst-case propagation of a withdrawn consent is therefore bounded only by token lifetime and an hourly poll.

A withdrawal that takes an hour to propagate is a poor fit for legal regimes whose operative triggers are knowledge and ease. GDPR Article 7(3) requires that withdrawal of consent be as easy as giving it. HIPAA's minimum necessary standard and audit controls assume that access decisions are contemporaneous with the request. When a passport still admits a researcher for fifty-nine minutes after the subject has withdrawn, the system has not failed to record the withdrawal. It has failed to make the withdrawal operative at the gate.

ERC-8356 does not replace GA4GH Passports. It supplies the missing status surface that a relying party can read at access time without trusting the issuer's endpoint. The instrument can still be a W3C Verifiable Credential whose termsOfUse reference a versioned template. The passport can still carry researcher identity and institutional affiliation. What moves on-chain is only the status anchor: ACTIVE, REVOKED_BY_SUBJECT, RENOUNCED_BY_GRANTEE, TERMINATED_BY_ISSUER, SUSPENDED, EXHAUSTED, SUPERSEDED. A status list fetched from an issuer-controlled endpoint can be rewritten or taken offline. A consensus-ordered revocation cannot. That is the only reason the status belongs on a chain at all.

FIGURE 2. GA4GH VISA PATH VERSUS ERC-8356 STATUS ANCHOR AT ACCESS TIME



TEXT SUMMARY (FIGURE 2)

Left path: GA4GH Visa Issuer issues a visa to a Passport Clearinghouse; the data gate learns of withdrawal only by polling, at best hourly. Right path: the subject calls revokeBySubject (or WithSig) on the ConsentGrant status anchor; the relying party gate reads isGrantActive or checkAccess at access time. ERC-8356 does not replace the visa; it makes withdrawal readable without trusting the issuer endpoint.

5. Design Principles

Six principles organize the specification. Each is stated here as an engineering constraint rather than as marketing language, because the standard is only as strong as the failures it forbids.

Principle 1. Three principals, never two. Subject, grantee, and optional agent are first-class fields. Collapsing any two into one is a non-conforming profile, not a simplification.

Principle 2. Status anchor, not instrument. The chain records authorization state. It does not store the human-readable terms, the subject's identity as an account address, or the biological data. The instrument is hashed (termsRef) as a versioned template shared across many subjects, never as a per-subject executed document.

Principle 3. Withdrawal is operative at access time. revokeBySubject is unconditional, immediate, and not blockable by the grantee, the issuer, or the contract operator. isGrantActive must return false for every descendant without requiring unbounded work in the revoking transaction. Lazy cascade is recommended precisely because an eager per-descendant write lets a grantee mint enough sub-grants to push withdrawal past the block gas limit.

Principle 4. The agent leg is independently revocable. revokeAgent kills only the agent. The human grant survives. That is the incident response primitive that two-party standards cannot express when a session key or tool provider is compromised.

Principle 5. Purpose is bound, and an unset registry fails closed. purposeCode indexes a registry that pins ontology releases. subGrant may narrow purpose only through registered narrowing. Where purposeRegistry() returns the zero address, subGrant requires exact purpose equality. Free-text purpose strings are forbidden on-chain.

Principle 6. Privacy is a correctness property. The privacy rules bind an implementation exactly as the rest of the Specification does. An implementation may satisfy every other requirement, function correctly, and still place its operator in breach of data protection law if it writes personal identifiers on-chain. subjectCommit is a per-grant commitment to a subject key, never a stable address, and bare hashes of enumerable address spaces are forbidden.

> HONESTY CONSTRAINT
>
> usesMax is a contractual ceiling the constrained party self-reports through commitUsage. It is not a cryptographic bound. A relying party that needs a bound the grantee cannot under-report must meter access outside this mechanism. The specification states that limit rather than advertising usesMax as stronger than it is.

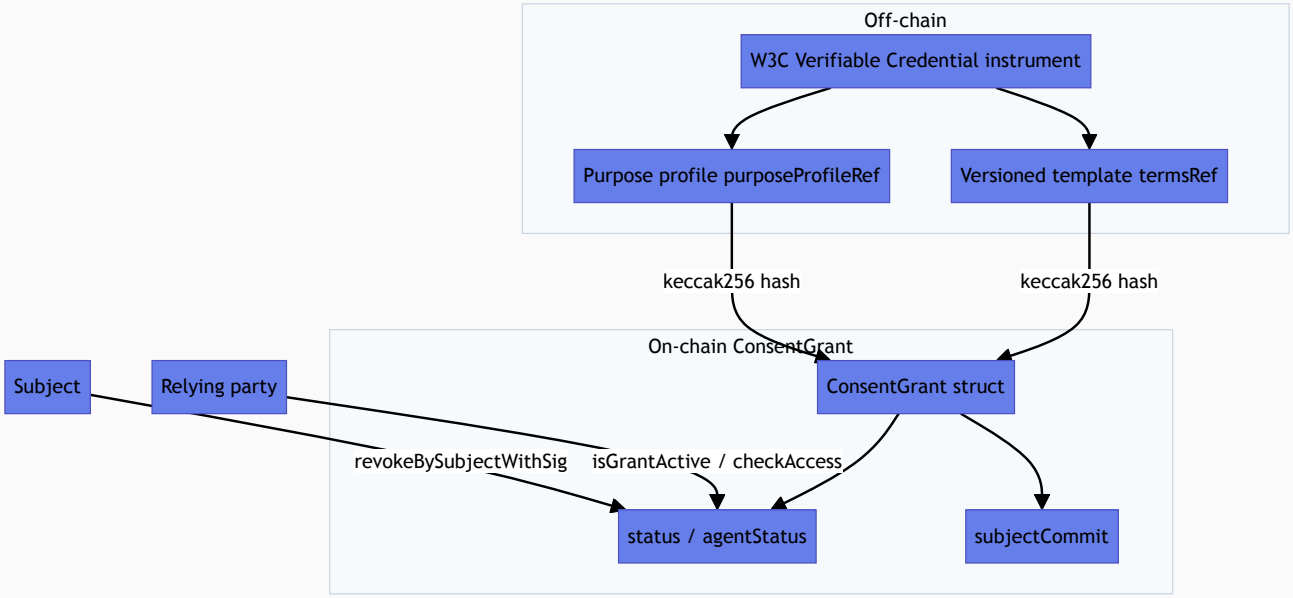
6. Architecture: Status Anchor and Off-Chain Instrument

A signature proves control of a key, not that a particular human assented. Whether an authorization is valid also turns on facts a contract cannot observe, including whether the signer had authority to act for the subject and whether any material representation in the instrument was false. Adjacent work reached the same conclusion. ERC-8328 states that its stored records are "attributable assertions, not proof that the reported action occurred or was lawful." ERC-8226 marks its own legal-text pointer as non-normative "since its content is not verifiable on-chain." ERC-8356 therefore claims weight as evidence and ordering, not as legal operative effect, with one exception: revocation status, which relying parties read directly and which is operative for them.

The instrument is carried as a W3C Verifiable Credential or equivalent off-chain document. termsRef MUST hash the versioned template referenced from the credential's termsOfUse, never the per-subject credential instance. Hashing the instance would be a commitment to personal data and is forbidden by Privacy rule 5. purposeProfileRef hashes a canonical purpose profile document, a JSON object under RFC 8785 with an array of term and value pairs that MUST be sorted by term before canonicalization so equal profiles hash equally.

Grants are soulbound. A transferable consent grant is a right of access that can be sold to a person's data. Consent runs to a named recipient; non-assignment is the property, not a limitation. Delegation is expressed by attenuated subGrant, which cannot exceed its parent and cascades on revocation through isGrantActive's ancestor walk.

FIGURE 3. STATUS ANCHOR VERSUS OFF-CHAIN INSTRUMENT



TEXT SUMMARY (FIGURE 3)

On-chain: grantId, subjectCommit, grantee, agent, purposeCode, ops, window, usesMax, status, and hashes of the off-chain instrument and purpose profile. Off-chain: the human-readable terms template, credentials, and usage records. The chain is a status anchor; the instrument never lands on-chain.

7. Data Model and Principals

The ConsentGrant storage layout occupies eight recommended slots. Field order is recommended rather than required; reordering costs gas without changing behaviour. Calldata encoding of the input struct is an implementation choice constrained by EVM stack limits: a full-width external struct may not compile even with the IR pipeline. The reference implementation packs seven small scalars into a single policy word with encodePolicy and decodePolicy helpers.

Status values are NONE, ACTIVE, REVOKED_BY_SUBJECT, RENOUNCED_BY_GRANTEE, TERMINATED_BY_ISSUER, SUSPENDED, EXHAUSTED, and SUPERSEDED. AgentKind values are NONE, SESSION_KEY, EXTERNAL_REGISTRY (for example ERC-8004), TOKEN_BOUND_ACCOUNT (ERC-6551), and ASSERTED_UNVERIFIED. ASSERTED_UNVERIFIED exists so that an unproven claim can be recorded honestly rather than disguised as a principal. It MUST NOT satisfy an agent constraint in checkAccess.

Flags include FLAG_SCOPE_IS_ROOT, FLAG_DELEGABLE, and FLAG_DESTROY_DERIVATIVES. Ops bits are fixed and normative: READ, QUERY, DERIVE, EXPORT, TRAIN. An unrecognized bit MUST NOT be treated as granting anything. Fixed values matter because a grant minted by one party is evaluated by another; independently assigned indices collide and the failure direction is disclosure.

subjectCommit is the only on-chain reference to the subject. It MUST be formed as keccak256(abi.encode(subjectSalt, subjectKey)), where subjectSalt is at least 128 bits of entropy, unique to the grant, and never written on-chain, and subjectKey is the address whose signatures authorize every subject-authored act for that grant. A bare keccak256(subjectKey) without a salt is forbidden because an address space is enumerable. A fresh subjectKey SHOULD be generated per grant so that a long-lived wallet address is not the opening. subjectOf(grantId) is published so the zero-subject profile is buildable for deployments that derive subject authority from an asset registry rather than from an on-chain commitment.

PRINCIPAL	ROLE	ON-CHAIN REPRESENTATION
Subject	Consents; data is about them; not the beneficiary	subjectCommit (never bare address)
Grantee	Authorized to exercise the grant	address grantee
Agent	Optional executor for the grantee	address agent + agentKind + agentStatus
Agent operator	Accountable organization for the agent	Off-chain; may call revokeAgent

8. Purpose Binding and Fail-Closed Registries

Purpose vocabularies used in practice are classification systems with parent and child terms. Equality over a free hash produces false denials: a grant for a broad permitted use will not match a request labelled with a narrower one that the ontology says it permits. ERC-8356 therefore specifies coarse equality over registered codes on-chain, with hierarchy reasoning performed

off-chain by the relying party, and requires the registry entry to pin the ontology release so a code's meaning cannot drift.

The registry interface is minimal and intentional:

```
interface IPurposeRegistry {
    function isNarrowing(uint32 childCode, uint32 parentCode) external view returns (bo
}
```

Where purposeRegistry() returns the zero address, subGrant MUST require exact purpose equality. An unset registry fails closed. Ontology subsumption reasoning is explicitly out of scope for the on-chain path. That is not a weakness. It is a refusal to put a full reasoner inside the EVM and a requirement that the relying party own the semantics it claims to enforce.

purposeProfileRef carries the hash of the full canonical profile, including parameters, because several widely used modifiers are parameterized. A disease-specific permission needs a disease. A geographic restriction needs a region. A time limit needs a duration. The profile document is a JSON object canonical per RFC 8785, containing an array of term and value pairs where term is an ontology IRI and value is absent or an IRI or literal. RFC 8785 does not reorder array elements, so implementations MUST sort the array by term ascending as UTF-8 byte order before canonicalization, and MUST reject profiles whose array is not so sorted.

9. The Independently Revocable Agent Leg

Incident response for regulated data almost never wants to destroy the human relationship. It wants to contain a compromised runtime. A research fellow should retain their grant after a lab's MCP server is rotated. A clinician should retain access after a stolen session key is revoked. Two-party mandates cannot express that distinction because the agent is modeled as the principal's extension rather than as a separate seat with its own status.

ERC-8356 stores agentStatus independently of status. revokeAgent is callable by the grantee, the agent, or the agent operator, so containment does not require the grantee to be reachable when the agent itself is the one reporting compromise. After revokeAgent, isGrantActive may still

return true for the human grant, while checkAccess fails for the revoked agent. The human can re-bind a new agent without minting a new root grant, subject to the implementation's agent update rules, or leave the grant agent-less so that only the grantee address satisfies checkAccess when agentKind is NONE.

ASSERTED_UNVERIFIED is the honest label for a claimed-but-unproven agent identity. It is recorded for audit. It never satisfies an agent constraint. That prevents the common failure mode in which a free-form string or an unauthenticated address is treated as if it were a principal.

> **CHECKACCESS AND ETH_CALL**
>
> checkAccess authenticates only an on-chain caller through msg.sender. An off-chain relying party that invokes it through eth_call supplies from itself and obtains no authentication whatsoever. Off-chain enforcement MUST combine isGrantActive or effectiveStatus with an independent authentication of the agent or grantee, for example a signature over the access request, an ERC-8004 agent session, or a transport-level credential. On-chain gates in the same transaction remain sound because msg.sender is then the EVM caller.

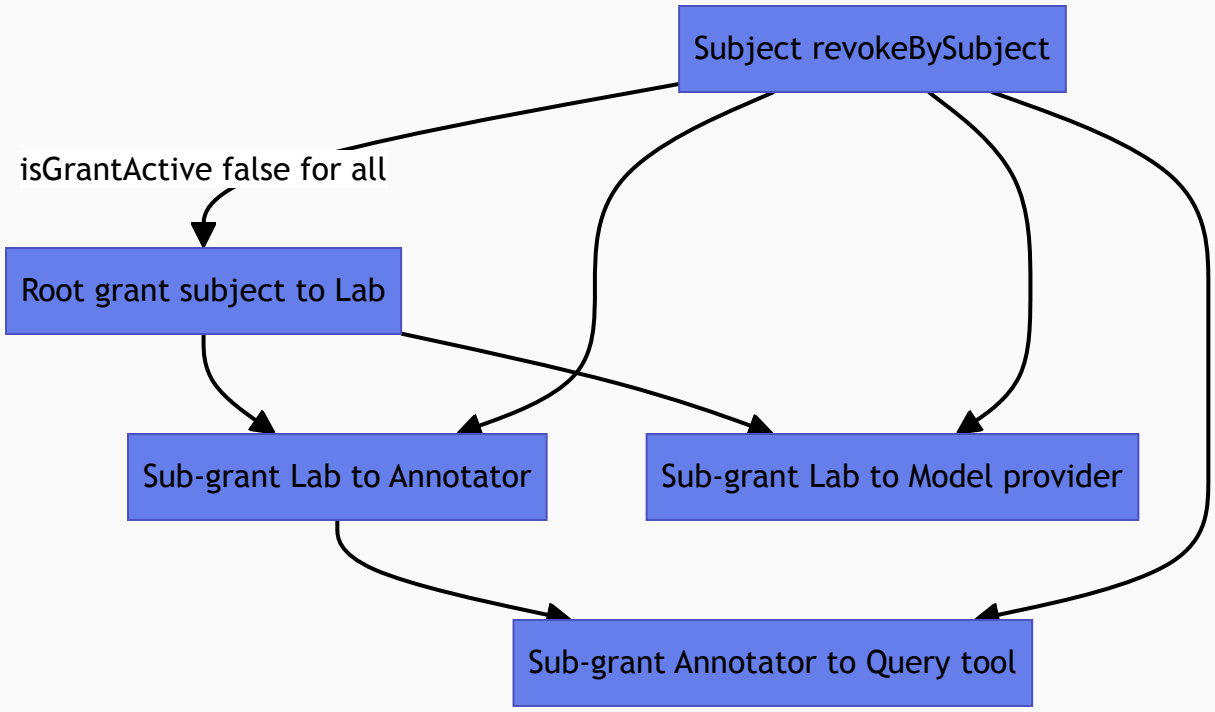
10. Attenuation and the Consent Graph

subGrant is the only legal widening of the network of parties who hold access, and it is not a widening of privilege. It MUST be called by the parent's grantee, and MUST revert unless the parent has FLAG_DELEGABLE set and all of the following hold: child subjectCommit equals parent subjectCommit; child ops is a subset of parent ops; child expiresAt is not later than the parent's; child notBefore is not earlier than the parent's; child usesMax does not exceed the parent's (where 0 means unlimited); child purposeCode is the parent's or a registered narrowing of it; and depth does not exceed the implementation's maxDepth.

Scope containment MUST be proven, not assumed. Subtree membership is not decidable from two 32-byte roots. Either the child names the same scopeRef as the parent, or the parent is root-scoped, the child is leaf-scoped, and scopeProof proves the child's scopeRef is a leaf under the parent's root. Accepting an unproven child scope voids attenuation entirely for Merkle-scoped grants: the grantee can mint a child naming any resource at all, and a later checkAccess on that child consults only the child's own scopeRef. That was a publication blocker fixed before the PR opened, and it remains the load-bearing negative test in the reference suite.

Merkle construction is normative so that two conforming implementations agree. Leaf is keccak256(bytes.concat(keccak256(resourceId))). Interior nodes use sorted-pair hashing. Empty proof is valid for a single-leaf tree. revokeScopeLeaf withdrawals MUST be consulted on every ancestor when evaluating a descendant, so a per-datum withdrawal survives a delegation hop.

FIGURE 4. CONSENT GRAPH WITH ATTENUATION AND REVERSE CASCADE ON WITHDRAWAL



TEXT SUMMARY (FIGURE 4)

A root grant attenuates into sub-grants (lab to annotator, lab to model provider, annotator to query tool) that can never exceed the parent on scope, ops, expiry, purpose, or uses. Subject revokeBySubject at the root makes isGrantActive false for every descendant without rewriting child storage.

That graph is why the standard cannot be reduced to a boolean flag on a single token. Consent has to travel with the artifact and narrow as it goes. Withdrawal has to reverse the graph without requiring the subject to find every child. isGrantActive walks ancestors. effectiveStatus reports the first terminal status inherited from an ancestor for display. The revoking transaction stays O(1).

11. Privacy Rules as Correctness Properties

The privacy section of ERC-8356 is not advisory. It binds an implementation exactly as the rest of the Specification does. An implementation may satisfy every other requirement, function correctly, and still place its operator in breach of data protection law.

The chain records authorization state, never facts about the person. The following MUST NOT be written to chain state or events: any identifier that carries meaning outside this protocol, in any form, including hashed and including encrypted (with the single permitted exception of the per-grant subject commitment); an unsalted hash of any identifier drawn from an enumerable space; data from which the underlying record can be reconstructed; date elements finer than a year and geography finer than a coarse region; the plain-language instrument text as a per-subject document; free-text purpose or condition strings; a stable subject identifier reused across grants; and session or behavioral identifiers.

Per-access events are prohibited for this reason. An event stream keyed to a subject publishes an access-pattern timeline. Access frequency and timing are themselves revealing, and on a permissioned chain with a known participant set they are attributable. The hash-chain-plus-commitment design preserves tamper-evidence and ordering over the records that were appended, while publishing only a periodic head and a count. It does not prove that every access was recorded. Completeness is not a free property of a self-declared usage log.

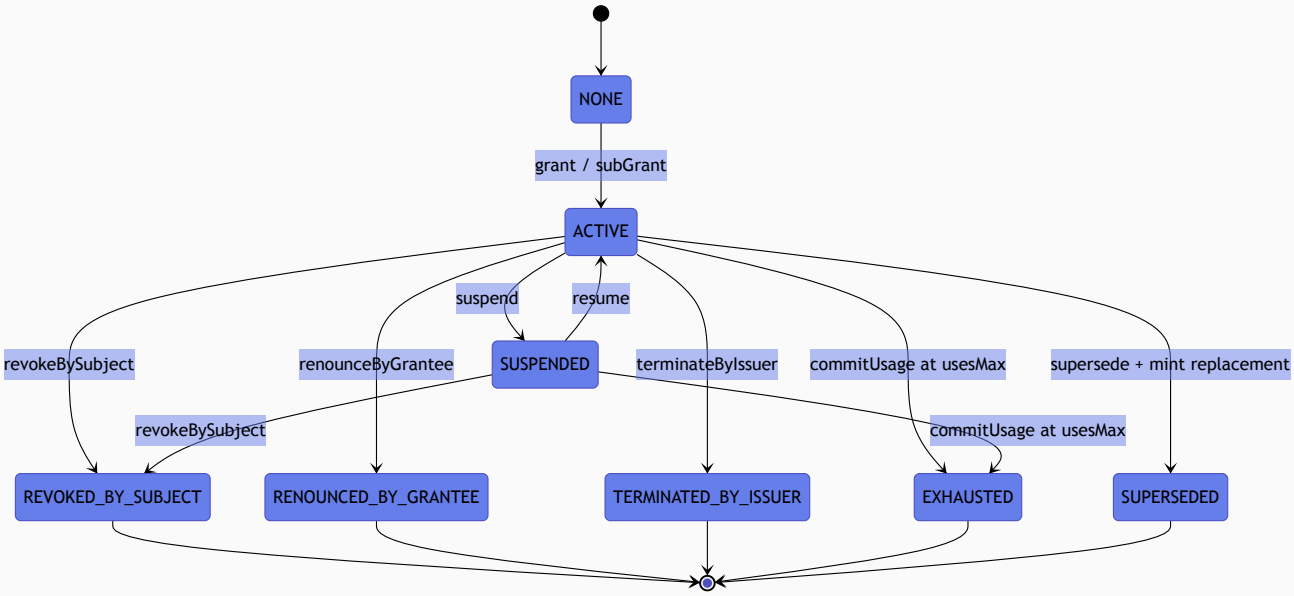
Deployments SHOULD prefer a permissioned network with an identifiable operator because it permits a clear allocation of controller responsibility. On a permissionless network there is a live argument that validators become joint controllers of the personal data in the state and logs they process. The governing constraint is simple: if a deployment cannot render every on-chain artifact anonymous by deleting off-chain material, then consent may not be an available lawful basis for it in some jurisdictions. Implementers SHOULD verify that this holds before relying on consent, rather than after.

> **SUBJECTCOMMIT LIMIT, STATED RATHER THAN FOUND**
>
> subjectCommit is a pseudonym, not anonymisation. It remains personal data while it can be linked to a person, and the erasure argument rests on destroying the key, not on the commitment being free of linkage. It hides the subject from observers, not from the grantee, who holds the credential.

12. Lifecycle, Revocation, and Status Transitions

Every non-NONE status value has exactly one writing path. Values with no path are dead weight and invite non-conforming custom setters. The transition table is part of the normative text of the ERC and is restated here for the whitepaper audience.

FIGURE 5. STATUS MACHINE (TERMINAL STATES HAVE NO RETURN TO ACTIVE)



TEXT SUMMARY (FIGURE 5)

NONE mints only to ACTIVE. From ACTIVE: subject revoke, grantee renounce, issuer terminate, suspend, exhaust at usesMax, or supersede with a replacement mint. SUSPENDED may resume to ACTIVE or still be revoked by the subject. Terminal states (REVOKED_BY_SUBJECT, RENOUNCED_BY_GRANTEE, TERMINATED_BY_ISSUER, EXHAUSTED, SUPERSEDED) never return to ACTIVE; re-grant mints a new grantId.

FROM	TO	WRITER	NOTES
NONE	ACTIVE	grant / subGrant	only mint path
ACTIVE	REVOKED_BY_SUBJECT	revokeBySubject / WithSig	terminal
ACTIVE	RENOUNCED_BY_GRANTEE	renounceByGrantee	terminal
ACTIVE	TERMINATED_BY_ISSUER	terminateByIssuer	terminal; issuer role implementation-defined

FROM	TO	WRITER	NOTES
ACTIVE	SUSPENDED	suspend	grantee or agent operator only
SUSPENDED	ACTIVE	resume	only the party that called suspend
SUSPENDED	REVOKED_BY_SUBJECT	revokeBySubject / WithSig	subject always wins
ACTIVE or SUSPENDED	EXHAUSTED	commitUsage	when cumulative uses reach usesMax
ACTIVE	SUPERSEDED	supersede path	MUST mint replacement in same transaction

REVOKED_BY_SUBJECT, RENOUNCED_BY_GRANTEE, TERMINATED_BY_ISSUER, EXHAUSTED, and SUPERSEDED are terminal. An implementation MUST NOT provide any function that returns a terminal grant to ACTIVE. Re-granting MUST mint a new grant with a new identifier. The sole exception to no-reinstatement is resume of SUSPENDED to ACTIVE, and it exists only so incident response can lift a temporary hold without erasing a later subject withdrawal.

Relayed withdrawal is mandatory. An implementation MUST accept a subject-signed revocation submitted by a third party (revokeBySubjectWithSig, revokeScopeLeafWithSig), so that a subject holding no fee token can withdraw. A design where granting accepts a relayed signature and withdrawal does not is non-conforming, because it makes withdrawal strictly harder than granting. That is the operational expression of GDPR Article 7(3) on-chain.

revocationEpoch MUST increase on every revocation of any kind. Relying parties that cache authorization decisions SHOULD re-validate when it changes. That bounds revocation latency without requiring per-access reads, and it is the answer to the GA4GH hourly poll without requiring a push channel into every clearinghouse.

13. Usage Accounting Without Per-Access Events

Implementations MUST NOT emit a per-access event. Usage is recorded off-chain as an append-only hash chain whose head is committed periodically via commitUsage. The chain is normative so that two parties can recompute the same head: H is keccak256; h0 is bytes32(0); hi = keccak256(abi.encodePacked(h(i-1), record_i)); each record_i is keccak256(abi.encode(grantId, accessedAt, op, resourceHash, requestId)).

commitUsage asserts that after count records in an epoch, the chain head is headHash. count MUST be monotonic. When usesMax is non-zero and count reaches usesMax, status becomes EXHAUSTED and MUST NOT overwrite a terminal subject or issuer status. That last rule closed a laundering path in which a grantee could erase REVOKED_BY_SUBJECT by driving the grant to EXHAUSTED after withdrawal.

usesMax is not a cryptographic bound. Only the grantee or agent can advance the off-chain chain and call commitUsage, so the party constrained by usesMax is also the party that reports use. The field is a contractual ceiling with on-chain accounting the constrained party self-declares. A relying party that needs a bound the grantee cannot under-report MUST meter access outside this mechanism, for example by serving bytes only through a gate that increments its own counter, or by requiring a third-party notary to call commitUsage. Implementations MUST document that honesty assumption wherever they surface usesMax to a subject.

What the chain provides is tamper-evidence and ordering over the records that were appended. It does not provide completeness. A party that declines to append a record leaves no gap a third party can detect from the head alone. The whitepaper states that limit in the same register as the specification, because overselling usage logs is how systems produce false assurance.

14. Regulatory Mapping

ERC-8356 is not a compliance product and does not claim to make any particular processing lawful. It is a technical substrate that maps cleanly onto several operative requirements when the surrounding organization does its legal work honestly.

GDPR Article 7(1). Demonstrable consent is supported by the subject's EIP-712 authorship of the grant and by the off-chain instrument hashed in termsRef. The chain proves that a signature existed and when; the organization still owns the quality of the information given to the subject.

GDPR Article 7(3). Withdrawal as easy as giving consent is supported by revokeBySubjectWithSig, which lets a subject with no fee token and no wallet gas withdraw through a relayer, and by the unconditional character of revokeBySubject.

GDPR Article 17. Right to erasure cannot be satisfied by an immutable chain that stores personal data. ERC-8356 therefore forbids writing personal data on-chain (with the narrow, per-grant subjectCommit exception) and treats erasure as destruction of off-chain keys and instruments. Where deletion of model weights is impossible, the standard refuses to pretend otherwise and leaves measurement and accounting as the honest remainder.

HIPAA §164.312(b). Audit controls map to the usage hash chain and to consensus-ordered status changes, not to a per-access event stream that would itself be a disclosure of access patterns.

CCPA and sale of data. Soulbound grants and non-assignment close the structural path by which a consent token becomes a transferable right of access. That is not a full CCPA analysis. It is a technical refusal to mint a sellable access token.

The privacy rules also recommend permissioned deployment with an identifiable operator. GenoBank.io's Sequentia network (chain ID 15132025) is that kind of network: a specialized L1 for genomic federation where controller responsibility is allocable. The reference ConsentGrant is deployed there alongside Avalanche for redundancy and public verification of the same bytecode shape.

15. Reference Implementation and Test Posture

The reference ConsentGrant contract is implemented in Solidity 0.8.28 with OpenZeppelin ERC-1155, EIP-712, and MerkleProof components. Runtime size on the open-item revision is 16,892 bytes. Source lives in the GenoBank.io contracts repository at `contracts/ConsentGrant.sol` (Genobank/biorouter-contracts). Forty-eight tests, mostly negative, assert the load-bearing failures: a sub-grant cannot exceed its parent on scope, ops, expiry, purpose, or uses; a claimed-but-unproven agent identity never satisfies an agent constraint; revoking the agent leg leaves the human grant alive; suspension is the only non-terminal return to ACTIVE; revocation cost does not grow with the number of delegated children; commitUsage cannot launder a subject withdrawal into EXHAUSTED; and a revoked agent cannot still write usage.

Live smoke scripts (grant, checkAccess, suspend, resume, revokeBySubject) are checked into the same repository:

- `scripts/smoke-consent-grant-fuji.js` (Avalanche Fuji, chain 43113)
- `scripts/smoke-consent-grant-sequentia.js` (Sequentia, chain 15132025)

Deployments of the open-item revision (August 2026), with public verification where explorers support it:

CHAIN	ADDRESS	EXPLORER / VERIFIED SOURCE
Avalanche mainnet (43114)	`0x360ac376e20B4d930da810f7CeA935F52693a84C`	SnowTrace (verified)
Avalanche Fuji (43113)	`0xc92f9f1D68A445189Ad3ad28524186A11Be30DcA`	SnowTrace testnet (verified)
Sequentia (15132025)	`0xD526E4d6e449A091D18900DC9ACb183e9556F714`	Sequentia explorer (verified source + ABI)

Runtimes are not byte-identical across chains because each embedding includes its own contract address for EIP-712 and self checks. They share the same compiler artifact, selectors, and constants (MAX_DEPTH 4, purpose registry zero for fail-closed purpose equality). Prior instances remain live and are recorded as superseded; they lack suspend, resume, terminateByIssuer, and ancestor leaf inheritance, and must not be used for new integrations.

Both Fuji and Sequentia smokes have been executed end to end against the open-item deployments. That is the operational standard GenoBank.io holds itself to: the paper, the ERC, the bytecode, the smoke, and the explorer entry must not drift without a named supersession.

Operator checklist: relying-party enforcement

A gate that serves regulated bytes MUST NOT treat a green `eth_call` as authentication. Combine on-chain status with an independent proof of who is calling:

1. **Resolve the grant.** Load `grantId` from the request (or from a binding stored when the session was opened).
2. **Read status at access time.** Call `isGrantActive(grantId)` or `effectiveStatus(grantId)` on the ConsentGrant for the deployment you trust. Refuse if not ACTIVE (accounting for inherited terminal status on ancestors).
3. **Authenticate the caller off-chain or in-tx.** `checkAccess` only authenticates `msg.sender` in a real transaction. For off-chain gates, verify a signature over the access request, an ERC-8004 agent session, or a transport credential that maps to grantee or agent.
4. **Check purpose, ops, and scope.** Either call `checkAccess(grantId, purposeCode, ops, resource, scopeProof)` in the same transaction as the gated action, or re-implement the same predicates after authenticating the caller.
5. **Honor agent revocation independently.** If `agentStatus` is revoked, refuse the agent even when the human grant remains ACTIVE. Bind a new agent only under grantee authority.
6. **Watch `revocationEpoch`.** If you cache authorization, re-validate when the epoch advances. Do not invent an hourly poll as the only validity path.
7. **Meter uses honestly if you need a hard ceiling.** `usesMax` is a self-declared contractual ceiling. For a bound the grantee cannot under-report, increment your own counter at the byte gate (or require a notary `commitUsage`).
8. **Keep the instrument off-chain.** Store and present the human-readable terms referenced by `termsRef`; never write personal data into the status anchor.

16. Comparison Matrix

CAPABILITY	ERC-4907 / 5006	ERC-8226	ERC-8328	GA4GH AAI	ERC-8356
Third principal (subject ≠	No	No	Modeled, not	Yes (data subject)	Yes, first-class

CAPABILITY	ERC-4907 / 5006	ERC-8226	ERC-8328	GA4GH AAI	ERC-8356
beneficiary)			enforced		
Withdrawal operative at access time	Owner-controlled	Grant-time check	Assertion only	Hourly poll / optional none	Yes, consensus status
Independent agent revocation	No	No	No	N/A	Yes
Purpose bound on-chain	No	Metadata non-normative	No	Visa scopes	Yes, fail-closed registry
Attenuating sub-delegation	No	Limited	No	Clearinghouse policy	Yes, proven scope
Personal data on-chain	Owner address	Principal address	Subject identifiers risk	Off-chain	Forbidden except subjectCommit
Instrument storage	N/A	Non-normative pointer	Assertions	Visa JWT	Off-chain template hash

The matrix is not a claim that ERC-8356 replaces any of those systems. It is a claim that the three-party data consent case needs a standard of its own, and that composing with ERC-8226, ERC-8004, and W3C credentials is the intended path rather than subsumption.

17. Deployment Context: Sequentia and GenoBank.io

GenoBank.io operates Sequentia (chain ID 15132025) as a permissioned L1 for genomic federation, BioNFT provenance, and programmable licensing. The explorer at explorer.sequentias-test.genobank.io now indexes blocks and transactions, verifies contract source through an Etherscan-compatible API, and catalogs NFT types discovered on-chain:

ERC-721 collections including BioAgent, ClaraJobNFT, LabDeliveryReceiptNFT, and LabNFT v2; ERC-1155 multi-tokens including BioAssetVault, BioNFTCredentials, and ConsentGrant; and the BIOIP ERC-20. That catalog is the operational surface against which ERC-8356 grants are minted: a consent grant is recorded against an existing asset token so that consent appears in that asset's provenance.

Metamorphic Consent, GenoBank.io's product language for revocable BioNFT-mediated relationships, is the user-facing story. ERC-8356 is the standards-track substrate that makes the hard properties portable beyond a single vendor. BioFS remains the biological filesystem protocol for acquisition, processing, and biocid addressing. Nothing in ERC-8356 moves genomic bytes on-chain. The standard is a status and purpose layer over assets that already exist in a privacy-preserving storage and routing stack.

Cross-chain redundancy on Avalanche mainnet and Fuji exists so that public verifiers, auditors, and partners who do not run a Sequentia node can still inspect the same interface and run the same tests against public explorers. Permissioned deployment remains the privacy recommendation; public deployment is the transparency and portability recommendation. Both can be true for different operators of the same bytecode.

18. Worked Scenarios

Clinical second opinion with a temporary tool

A patient (subject) consents to a second-opinion clinic (grantee) for a purpose code corresponding to clinical evaluation of an existing molecular report. The clinic binds a session key (agent) for a contracted review platform. When the platform vendor reports a credential leak, the clinic calls revokeAgent. The human grant remains ACTIVE. The clinic binds a new agent under a new session key without asking the patient to re-sign the root instrument. If the patient later withdraws entirely, revokeBySubjectWithSig is submitted by a patient-advocacy relayer that holds no substantive authority, only gas. isGrantActive returns false for every descendant. The molecular report bytes never moved on-chain; only the status did.

Research cohort with attenuated annotation hop

A biobank (acting with subject-signed root grants) authorizes a research institution as grantee for a purpose code corresponding to non-commercial disease association research. The institution sub-grants to an annotation vendor with ops limited to READ and QUERY, a narrower expiry, and a Merkle-proven leaf scope covering only the VCF objects, not the BAM objects. The vendor cannot EXPORT. When a subject withdraws, the root status becomes REVOKED_BY_SUBJECT. The annotation vendor's next checkAccess fails without a separate notification channel, because isGrantActive walks the ancestor. The institution's sub-grant is not separately rewritten; the cascade is logical, not an unbounded storage walk.

Model training and the hard edge of erasure

A subject consents to a model provider for a purpose profile that includes TRAIN with FLAG_DESTROY_DERIVATIVES set for intermediate extracts. Intermediate vectors can be deleted when the grant ends. Model weights cannot be cleanly unlearned with today's techniques. ERC-8356 does not claim to reverse training. It requires honest accounting through commitUsage for the hops that can be measured, and it refuses to store personal data on-chain that would make the status surface itself a second privacy problem. The whitepaper and the standard both treat permanence of weights as a measurement problem rather than as a deletion promise the technology cannot honor.

Agent compromise without destroying the human relationship

A research fellow retains a grant. Their MCP server is rotated after an incident. revokeAgent is called by the agent operator. The fellow's grantee address still satisfies checkAccess when agentKind is reset or when a new SESSION_KEY is bound. The subject is not asked to re-consent merely because a tool broke. That separation is the entire point of an independently revocable agent leg.

Program closure without subject blame

A study ends. terminateByIssuer marks grants TERMINATED_BY_ISSUER. That terminal state is distinct from REVOKED_BY_SUBJECT, so later audits do not misread institutional closure as participant withdrawal. EXHAUSTED remains reserved for usage ceilings, not for politics or program calendars.

19. Open Items and Research Agenda

The PR and Magicians thread deliberately publish residual weaknesses rather than hiding them. usesMax remains a self-declaration by the constrained party. The usage hash chain has a named hash function and record schema, but completeness is still not free. Merkle leaf construction is now normative, including ancestor inheritance of revoked leaves. Status transitions are fully tabled, including suspend and resume. checkAccess's eth_call limitation is stated as a normative warning. termsRef is restricted to versioned templates. Purpose profile array ordering is fixed for RFC 8785 stability.

Research and engineering work that remains useful includes: a recommended purpose ontology profile for clinical and research genomics that maps cleanly onto DUO and related vocabularies; a standard composition pattern with ERC-8004 agent sessions for off-chain checkAccess authentication; wallet UX for EIP-712 payloads that currently pack seven scalars into one word; formal verification of the attenuation and cascade invariants; and measurement protocols for the hard edge where model weights cannot be erased. GenoBank.io will continue to ship negative tests and supersede vulnerable deployments rather than leave them unlabeled.

20. Conclusion

ERC-8356 standardizes the three-principal case that every data consent decision actually is: a subject who consents, a grantee who benefits, and an optional agent that exercises access. It makes withdrawal operative at access time without storing the instrument or the person on-chain. It binds purpose through a fail-closed registry. It gives incident response an independently revocable agent leg. It composes with existing agent and credential standards rather than pretending to replace them.

For GenoBank.io, the standard is the portable form of Metamorphic Consent. For the Ethereum ecosystem, it is a missing Standards Track interface for regulated data in the age of software agents. For patients and research participants, it is a technical commitment that withdrawal is not a comment in a log, but a status every honest gate must read before it serves the next byte.

The claim has been opened for public review as ethereum/ERCs pull request 1921 and discussed on Ethereum Magicians thread 29217. Implementations, critiques, and purpose ontology

proposals are welcome. The test suite is mostly negative for a reason: a consent system that grants correctly but revokes late is worse than no consent system, because it produces an audit trail that looks authoritative and is not.

RELATED GENOBANK.IO WHITEPAPERS

- Sequentia Network, L1 context for genomic federation, BioNFT, and programmable licensing (chain 15132025).
- BioFS Protocol, biological filesystem, biocid addressing, and federated discovery under consent.
- BioNFT and ensilicated genomes, patient-owned BioNFT substrate Metamorphic Consent builds on.
- GA4GH Passport 2.0 blockchain architecture, passport / visa mapping to on-chain grants and BioNFTs.
- GA4GH, BioNFT, and Sequentia, operational bridge between GA4GH AAI and GenoBank.io deployment.
- All whitepapers

SUGGESTED CITATION

Uribe, D. (2026). *ERC-8356: Purpose-Bound Third-Party Data Consent* (Technical whitepaper, v1.0). GenoBank.io. https://genobank.io/whitepapers/erc-8356-purpose-bound-consent/ Same work as ethereum/ERCs pull request 1921 and Ethereum Magicians thread 29217. PDF snapshot: erc-8356-purpose-bound-consent.pdf. A Zenodo DOI may be minted for archival citation of a frozen PDF; until then, cite the URL and PR number.

21. References

1. Uribe, D. ERC-8356: Purpose-Bound Third-Party Data Consent. ethereum/ERCs pull request 1921, 2026. https://github.com/ethereum/ERCs/pull/1921
2. Uribe, D. Ethereum Magicians discussion for ERC-8356. Thread 29217. https://ethereum-magicians.org/t/erc-8356-purpose-bound-third-party-data-consent/29217

3. Entriken, W. and Uribe, D. Biosample permission token with non-fungible tokens. 2020.
4. Uribe, D. and Waters, G. Privacy Laws, Genomic Data and Non-Fungible Tokens. Journal of the British Blockchain Association, 2020.
5. Ethereum ERC-8226: Regulated Agent Mandate (Draft).
6. Ethereum ERC-8328: Subject-Linked Compliance Event Log (Review).
7. Ethereum ERC-8004: Trustless Agents (Draft).
8. Ethereum ERC-4907 and ERC-5006: rental and time-bounded user roles (Final).
9. W3C. Verifiable Credentials Data Model 2.0. Recommendation, 2025.
10. GA4GH. Authentication and Authorization Infrastructure (AAI) profile and Passport / Visa specifications.
11. Regulation (EU) 2016/679 (General Data Protection Regulation), Articles 7 and 17.
12. U.S. HIPAA Security Rule, 45 C.F.R. §164.312.
13. RFC 8785. JSON Canonicalization Scheme (JCS).
14. RFC 2119 and RFC 8174. Key words for use in RFCs to Indicate Requirement Levels.
15. GenoBank.io. Sequentia Network whitepaper and BioFS / Metamorphic Consent documentation. https://genobank.io/whitepapers/
16. GenoBank.io. Reference implementation: ConsentGrant.sol and smoke scripts. https://github.com/Genobank/biorouter-contracts
17. SnowTrace verified ConsentGrant (Avalanche mainnet). https://snowtrace.io/address/0x360ac376e20B4d930da810f7CeA935F52693a84C#code
18. SnowTrace verified ConsentGrant (Avalanche Fuji). https://testnet.snowtrace.io/address/0xc92f9f1D68A445189Ad3ad28524186A11Be30DcA#code
19. Sequentia Network Explorer verified ConsentGrant. https://explorer.sequentias-test.genobank.io/address/0xD526E4d6e449A091D18900DC9ACb183e9556F714

Links: PR 1921 · Magicians 29217 · ConsentGrant.sol · Sequentia · Avalanche mainnet · Fuji · PDF · All whitepapers